

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Alain ROSSMANN, et al
Title: Method and Architecture for Providing Pervasive Security to
Digital Assets
Serial No.: 10/076,254
Confirmation No.: 8579
Filing Date: 02/12/2002
Examiner: N/A
Group Art Unit: 2161
Docket No: SS-004

RECEIVED

SEP 10 2002

Technology Center 2100

September 4, 2002

RESPONSE TO DECISION ON PETITION BY APPLICANT
and
REQUEST FOR RECONSIDERATION

Commissioner for Patents
Attention: Mr. Pinchus K. Laufer
Box Technology Center 2100
Washington, DC 20231

Dear Sir:

This is to respond to DECISION ON PETITION FOR ACCELERATED EXAMINATION UNDER MPEP§708.02(VIII) dated July 09, 2002. The DECISION states that the PETITION is deficient for the following reasons:

- Failure to provide a listing of the field of search by class and subclass; and
- Failure to provide a detailed description of how claimed subject is patentable over each reference. Applicant has merely reproduced the abstracts (or a portion thereof) provided in each reference. This is no detailed discussion of the references as required by section (e) to the extent required by 37 CFR 1.111(b) and (c).

*REFERENCE
To 7/9/02
DECISION IS
EXHIBITED.
According to
ATTY, NO DECISION
IN THIS CASE
(UNITED STATES
COURT)*

Accordingly, the Applicants hereby submit that the pre-examination patent search was initially confined to two classes 380/23 and 713/200, and then expanded into other classes.

The Applicants respectfully disagree with the conclusion of the Examiner that "Applicant has merely reproduced the abstracts (or a portion thereof) provided in each reference". In fact, the references listed as U-V5 have no abstracts. Nevertheless, the Applicants submit herewith a **supplemental STATEMENT OF PRE-EXAMINATION SEARCH AND DISCUSSION OF REFERENCES DEEMED MOST CLOSELY RELATED TO SUBJECT MATTER ENCOMPASSED BY THE CLAIMS** to provide the information the Examiner has deemed missing from the PETITION originally filed June 10, 2002.

According to the DECISION ON PETITION TO MAKE SPECIAL, the submission herewith is believed to have overcome the two items which the Examiner relied upon to dismiss the PETITION. Hence the Applicant believes that the PETITION shall be granted. Please telephone the undersigned at (408)777-8873, if there are any questions.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner of Patents and Trademarks, Attention: Petition Special, Washington, DC 20231", on September 5, 2002.

Name: Joe Zheng

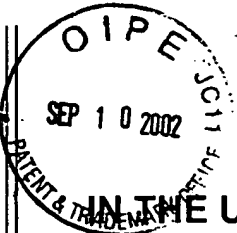
Signature: Joe Zheng

Respectfully submitted;



Joe Zheng

Reg. No.: 39,450



2161

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Alain ROSSMANN, et al
Title: Method and Architecture for Providing Pervasive Security to Digital Assets
Serial No.: 10/076,254
Confirmation No.: 8579
Filing Date: 02/12/2002
Examiner: N/A
Group Art Unit: 2161
Docket No: SS-004

RECEIVED
SEP 16 2002
Technology Center 2100

September 4, 2002

Supplemental

**STATEMENT OF PRE-EXAMINATION SEARCH AND DISCUSSION OF
REFERENCES DEEMED MOST CLOSELY RELATED TO SUBJECT MATTER
ENCOMPASSED BY THE CLAIMS**

Commissioner for Patents
Attention: Mr. Pinchus M. Laufer
Box Technology Center 2100
Washington, DC 20231

RECEIVED
SEP 18 2002
GROUP 3600

Dear Sir:

In support of the enclosed **RESPONSE TO DECISION ON PETITION BY
APPLICANT and REQUEST FOR RECONSIDERATION**, the Applicants provide hereinafter a supplemental detailed description of the submitted references that are deemed most closely related to the subject matter, or subject matters of the claims presented in a preliminary amendment filed earlier.

The following supplemental detailed description is provided in reference to the item numbers in the PTO Form-1449 filed earlier:

Para. 1: **B. C. and D.** US Patent No.: 5,276,735, US Patent No.: 5,499,297 US Patent No.: 5,502,766 to Boebert et al, sharing substantially the similar specification, disclose a data communication system providing for the secure transfer and sharing of data via a local area network and/or a wide area network. In particular, see FIG. 14, the system uses what is called processing elements to generate a variety of data elements (keys, identifiers, and attributes) to identify and authenticate the user, assign user security access rights and privileges, and assign media and device attributes to a data access device according to a predefined security policy. Thus it is provided a trusted path for communication between a workstation and a secure computer over an untrusted communication medium. Although a secured link with a client machine is being sought to be established in the subject matters of the claims, Boebert does not teach or suggest the use of the electronic data secured in a format including security information and an encrypted data portion, the security information including access rules and controlling restrictive access to the encrypted data portion.

Para. 2: **H. and S2.** US Patent No.: 5,933,498 and US Patent No.: 6,314,409 B2 to Schneck, et al., sharing the substantially similar specification, discloses a method and device provided for controlling access to data. As shown in FIG. 2, the logic data structure for includes an encrypted body part 120, an unencrypted body part 122, encrypted rules 124 (if provided with the packaged data), and encrypted ancillary information 126. Encrypted rules 124 are an encrypted version of access rules 116. According to lines 64-66 of Col. 10, the rules 116 further include an encrypted data key 138 as well as the actual rules. However, Schneck fails to teach or suggest that the electronic data is secured in a format including security information and an encrypted data portion, the security information including access rules and controlling restrictive access to the encrypted data portion, and, a user key of a user is

activated, after the user is authenticated, wherein the user key is used to access the access rules in the security information.

Para. 3: L. US Patent No.: 6,098,056 to Rusnak, et al. discloses a system and method for limiting access to and preventing unauthorized use of an owner's digital content stored in an information network and available to clients under authorized conditions. More specifically shown in FIG. 5, when a client accesses a server to acquire a digital content encrypted in a Document Encryption Key (DEK), the server encrypts the DEK with the server's public key, using a public/private key pair algorithm and places the encrypted content in a digital container for storing and transferring information in a secure manner. The client's workstation is coupled to the server for acquiring the limited access digital content under the authorized condition. A Trusted Information Handler (TIH) is validated by the server after the handler provides a data signature and type of signing algorithm to transaction data. After the handler has authenticated, the server decrypts the encrypted DEK with its private key and re-encrypts the DEK with the handler's public key ensuring that only the information handler can process the information. The encrypted DEK is further encrypted with the client's public key personalizing the digital content to the client. The client's program decrypts the DEK with his private key and passes it along with the encrypted content to the handler which decrypts the DEK with his private key and proceeds to decrypt the content for displaying to the client. However, Rusnak does not teach or suggest that the content is secured in a format including security information and an encrypted data portion, the security information including access rules and controlling restrictive access to the encrypted data portion.

Para. 4: S. US Patent No.: 6,272,632 B1 to Carman, et al. discloses a system and method for data recovery. As shown in FIG. 10, a file structure includes a header 1010 and an encrypted payload 1020. The header 1010 includes key recovery center (KRC) identifier field 1011 and key identifier field 1012. The combination of values in the KRC identifier field 1011 and key identifier field 1012 uniquely identifies the KRC and a key recovery center (KRC) public key

(KRCpub). KRCpub used to encrypt the payload section 1020. Accordingly, an encrypting system encrypts data using a secured key (KS) to produce encrypted data or a cipher text. The encrypting system then generates a key recovery field (KRF). The KRF includes an access rule index (ARI) and the KS. The KS is protected by a key recovery center (KRC) public key (KRCpub). KRCpub is acquired in a registration phase. During this registration phase, an access rule defining system defines an access rule (AR) that controls subsequent access to the secret KS. After the KRC receives the AR from the AR defining system, the KRC returns an ARI. The ARI can be included in one or more KRFs attached to subsequent encrypted files. The ARI can be included in one or more KRFs attached to subsequent encrypted files. But Carman does not teaches that "establishing a secured link with a client machine when an authentication request is received from the client machine, the authentication request including an identifier identifying a user of the client machine to access the electronic data, wherein the electronic data is secured in a format including security information and an encrypted data portion, the security information including access rules and controlling restrictive access to the encrypted data portion, authenticating the user according to the identifier; and activating a user key after the user is authenticated, wherein the user key is used to access the access rules in the security information."

Para. 5: **S1.** and **S3.** US Patent No.: 6,289,450 B1 and US Patent No.: 6,339,825 B2 to Pensak, et al., sharing substantially similar specification, discloses a system for encrypting electronic information such as a document so that only users with permission may access the document in decrypted form. As detailed in FIG. 2 and its corresponding description, the process of encrypting the information includes selecting a set of policies as to who may access the information and under what conditions. A remote server 206 stores a unique identifier for the information and associates an encryption/decryption key pair and access policies with the information. Software components residing on the author's computer retrieve the

encryption key from the remote server, encrypt the information, and store the encrypted information at a location chosen by the author. When a user 208 wishes to access the information acquires the encrypted information electronically. The software components retrieve the associated decryption key and policies, decrypt the information to the extent authorized by the policies, and immediately delete the decryption key from the viewing user's computer upon decrypting the information and rendering the clear text to the viewing user's computer screen. Significantly different from what Pensak discloses, the claimed invention claims that the electronic data (i.e., the information) is secured in a format including security information and an encrypted data portion, the security information including access rules and controlling restrictive access to the encrypted data portion, and, a user key of a user is activated, after the user is authenticated, wherein the user key is used to access the access rules in the security information.

Besides the distinctions stated above, the claimed subject matter is further distinguishable with particularity over the above patents/publications by:

Claim 20's "authenticating a user attempting to access the electronic data; maintaining a private key and a public key, both associated with the user, wherein the electronic data, when secured, includes a header and an encrypted data portion, the header further includes security information controlling who, how, when and where the secured electronic data can be accessed and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme; encrypting the security information with the public key when the electronic data is to be written into a store; and decrypting the security information with the private key when the electronic data is to be accessed by an application."

Claim 31's "receiving a request to access the electronic data; determining security nature of the electronic data; when the security nature indicates that the electronic data is secured, the electronic data including a header and an

encrypted data portion, the header including security information controlling restrictive access to the encrypted data portion and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme, determining from the security information if the user has necessary access privilege to access the encrypted data portion; and decrypting the encrypted data portion only after the user is determined to have the necessary access privilege to access the encrypted data portion."

Claim 41's "a client machine executing a document securing module that operates in a path through which the electronic data is caused to pass when selected, the document securing module determining security nature of the electronic data, an access control server coupled to the client machine over a network, the access control server including an account manager managing all users who access the electronic data; and wherein the client machine and a user thereof are caused by the document securing module to be authenticated with the access control server when the security nature indicates that the electronic data is secured; and wherein access rules in the secured electronic data are retrieved with a user key associated with the user."

Claim 47's "a storage device including at least an active place designated for keeping the electronic data secured, the secured electronic data including encrypted security information that further includes at least a set of access rules and a file key, wherein the access rules, expressed in a descriptive language, protects the file key and controls restrictive access to the secured electronic data; a client machine coupled to the storage device and executing a document securing module operative to intercept the electronic data when the electronic data is caused to transport from the active place; an access control server coupled to the client machine over a network and receiving a part of the electronic data including the encrypted security information from the client machine, the encrypted security information being decrypted with a user key associated with a user attempting to access the electronic data after both the user and the client machine are authenticated; wherein the set of access rules

are measured against access privilege of the user in the access control server, if successful, the file key is returned to the client machine to facilitate a recovery of the electronic data in clear mode."

Claim 48's "program code for establishing a secured link with a client machine when an authentication request is received therefrom, the authentication request including an identifier identifying a user from the client machine to access the electronic data in a secured format including security information and an encrypted data, the security information including access rules and controlling restrictive access to the encrypted data portion; program code for authenticating the user according to the identifier; and program code for activating a user key after the user is authenticated, wherein the user key is used to access the access rules in the security information."

Claim 67's "program code for authenticating a user attempting to access the electronic data; program code for maintaining a private key and a public key, both associated with the user, wherein the electronic data, when secured, includes a header and an encrypted data portion, the header further includes security information controlling restrictive access to the encrypted data portion and protecting the private key and a public key by access rules therein; program code for encrypting the security information with the public key when the electronic data is to be written into a store; and program code for decrypting the security information with the private key when the electronic data is to be accessed by an application."

Claim 78's "program code for receiving a request to access the electronic data; program code for determining security nature of the electronic data; when the security nature indicates that the electronic data is secured, wherein the electronic data including a header and an encrypted data portion, the header including security information and the encrypted data portion is an encrypted version of the electronic data according to a predetermined encryption scheme, program code for determining from the security information if the user has

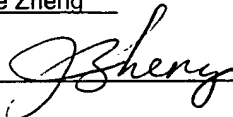
necessary access privilege to access the encrypted data portion; and program code for decrypting the encrypted data portion only after the access privilege of the user is permitted in view of the security information."

Hence, the applicants believe that claims 1, 20, 31, 41, 78, 48, 67, and 78 and thus their dependent claims also, are each patentable over the references discussed in paragraph Para. 1-5 above and related references listed in PTO Form 1449 filed earlier.

Please telephone the undersigned at (408)777-8873, if there are any questions.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner of Patents and Trademarks, Washington, DC 20231", on ~~June 6~~ 6/05 2002.

Name: Joe Zheng

Signature: 

Respectfully submitted;



Joe Zheng
Reg. No.: 39,450